UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2012 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. RYAN CLEARY, Defendant.	CR No. 12- CR12-0561 I N D I C T M E N T [18 U.S.C. § 371: Conspiracy; 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Unauthorized Impairment of a Protected Computer]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

1. The following definitions apply to this Indictment:

a. Botnet: A "botnet" is a collection of compromised computers, known as "bots," that autonomously respond to and execute commands issued by the botnet's owner, often for nefarious purposes. Computers become part of a botnet by being infected with malicious software, known as "malware," which may install itself on a user's computer without the user's knowledge, often by taking advantage of web browser vulnerabilities or by

tricking the user into running a Trojan horse program. Once the computer is infected and becomes a bot in the botnet, the malware can listen for, respond to, and execute commands issued by the botnet's owner, for example, to make connections to a particular server as part of a distributed denial of service, or "DDoS," attack.

b. DDoS attack: A "DDoS attack" is a type of malicious computer activity that attempts to render a computer resource unavailable to its intended users by flooding it with large amounts of data or commands. As a result, the victim computer is unable to handle legitimate network traffic, and legitimate users are denied the services of the computer resource. One common method of attack involves saturating the target computer with external communications requests, such that it cannot respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable. For example, a DDoS attack against a website server might flood the server with so many webpage requests that the server can no longer respond to legitimate traffic. Depending on the type and strength of the DDoS attack, the victim computer and its network may become completely disabled and unable to perform their intended functions without significant repair. A DDoS attack is "distributed" in nature if the flood of data and/or commands sent to the target machine originates from a large number of computers, for example, when the owner of a botnet directs all of the bots in the botnet to send requests to the same server at the same time.

2. At all times relevant to this Indictment:

a. DreamHost ("DreamHost"), a subsidiary of New Dream Network, LLC, was a data and server hosting company located within the Central District of California that provided shared, dedicated, and virtual private server hosting services to numerous individuals and businesses. DreamHost leased server space and computing resources for use by its clients, as well as provided Internet connectivity, typically in a data center. DreamHost maintained computer systems, including its own and those used to provide hosting services, in Los Angeles, California.

b. "Anonymous" was a collective of computer hackers and other individuals located throughout the world, including the United States, that conducted cyber attacks against individuals and entities that were perceived to be hostile to Anonymous and its members' interests. These attacks included, among other things, the theft and later dissemination of confidential information from victims' computer systems.

c. "Lulz Security," or simply "LulzSec," was a group of computers hackers affiliated with Anonymous. LulzSec conducted cyber attacks against the computer systems of various corporate and government entities in the United States and throughout the world.

d. Defendant RYAN CLEARY ("defendant CLEARY"), a resident and citizen of the United Kingdom, was a member of and affiliated with various hacking groups, including Anonymous and LulzSec.

i. Defendant CLEARY used the following online nicknames and usernames, and variants thereof, including, among others, "ryan," "herschel.mcdoogenstein," "anakin," "evanwarwick," "francis madsen," "george hampsterman," "ni," "viral," and "x."

ii. Defendant CLEARY developed software for, and maintained and controlled a large botnet, comprised of tens of thousands, and potentially hundreds of thousands, of bots. Defendant CLEARY used his botnet to conduct DDoS attacks against various corporate and government entities, including DreamHost. Defendant CLEARY also rented out his botnet for others to use, that is, individuals paid defendant CLEARY money in exchange for being able to conduct DDoS attacks against targets of their choosing using defendant CLEARY's botnet for a certain period of time.

iii. Defendant CLEARY assisted LulzSec in its hacking activities, including by identifying security vulnerabilities on victim computers, exploiting such vulnerabilities, conducting DDoS attacks, and also establishing and providing access to servers and other computer resources for LulzSec members to use, including to communicate amongst each other and to store and publish confidential information stolen from LulzSec's victims.

COUNT ONE

[18 U.S.C. § 371]

3. The Grand Jury re-alleges and incorporates by reference the introductory allegations set forth in paragraphs one and two of this Indictment.

A. THE OBJECT OF THE CONSPIRACY

4. Beginning in or about April 2011, and continuing through in or about June 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant CLEARY, together with others known and unknown to the Grand Jury, including members of LulzSec, knowingly combined, conspired, and agreed to intentionally cause damage without authorization to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

5. It was a part and an object of the conspiracy that defendant CLEARY, and others known and unknown to the Grand Jury, including members of LulzSec, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, by impairing the integrity and availability of data, a program, a system, and information on a computer system that was used in and affecting interstate and foreign commerce and communication, causing a loss to one or more persons or entities during a one-year period aggregating at least $5,000 in value.

B. THE MANNER AND MEANS OF THE CONSPIRACY

6. The object of the conspiracy was carried out, and to be carried out, in substance, as follows:

a. Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would identify security vulnerabilities in the computer systems of various corporate and government entities for the purpose of causing damage to and/or gaining unauthorized access to such systems.

b. Taking advantage of the identified security vulnerabilities, defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would cause damage to such computer systems.

c. Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would also hack into such computer systems to obtain confidential information.

d. Defendant CLEARY would provide LulzSec with access to servers and other computer resources to facilitate communication amongst LulzSec members and to store and publish information stolen from compromised computer systems.

e. Defendant CLEARY and other known and unknown co-conspirators, including members of LulzSec, would publish the stolen information online.

f. Defendant CLEARY would instruct an associate who had been contacted by law enforcement about LulzSec to falsely accuse another person of LulzSec's activities.

C. OVERT ACTS

7. In furtherance of the conspiracy, and to accomplish its object, defendant CLEARY, together with others known and unknown to the Grand Jury, committed and willfully caused others to commit the following overt acts, among others, in the Central District of California and elsewhere:

Overt Act No. 1: On or about April 20, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, hacked into the computer systems of Fox Entertainment Group, Inc. ("Fox"), a commercial broadcasting television company located within the Central District of California, and stole confidential information, including information relating to individuals registered to receive information regarding auditions on "The X-Factor," a Fox television show.

Overt Act No. 2: On or before May 29, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, hacked into the computer systems of the Public Broadcasting System ("PBS"), a non-profit public television broadcasting service, and defaced the website for the PBS news program "News Hour."

Overt Act No. 3: On or about June 2, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, hacked into the computer systems of Sony Pictures Entertainment, Inc. ("Sony Pictures"), a major motion picture and television production company located within the Central District of California, and stole confidential information relating to users who had registered on Sony Pictures' website.

Overt Act No. 4: On or about June 2, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, launched the website lulzsecurity.com.

Overt Act No. 5: On or about June 2, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, published on lulzsecurity.com information stolen from the computer systems of Fox.

Overt Act No. 6: On or about June 2, 2011, defendant CLEARY and his co-conspirators, including members of LulzSec, published on lulzsecurity.com information stolen from the computer systems of Sony Pictures.

Overt Act No. 7: On or about June 2, 2011, defendant CLEARY provided his co-conspirators, including members of LulzSec, access to computer resources located at QuadraNet, a data and server hosting company in the Central District of California, to facilitate communication between defendant CLEARY's co-conspirators and to store and publish stolen data.

Overt Act No. 8: On or before June 9, 2011, defendant CLEARY provided his co-conspirators, including members of LulzSec, access to computer resources located at GigeNET, a data and server hosting company in Illinois, to facilitate communication between defendant CLEARY's co-conspirators and to store and publish stolen data.

Overt Act No. 9: On or about June 10, 2011, defendant CLEARY instructed an associate who had been contacted by law enforcement regarding LulzSec to provide "disinformation" that "leads away from" LulzSec members; specifically, defendant CLEARY instructed the associate to falsely accuse M.D.M. of LulzSec's activities and offered to provide the associate with fake access logs pointing to M.D.M. to give to law enforcement.

Overt Act No. 10: On or about June 14, 2011, defendant CLEARY launched a DDoS attack against the servers hosting the online game League of Legends, owned and operated by Riot Games, Inc., located within the Central District of California.

Overt Act No. 11: On or before June 15, 2011, defendant CLEARY provided his co-conspirators, including members of LulzSec, access to computer resources located at Linode, a data and server hosting company in New Jersey, to facilitate communication between defendant CLEARY's co-conspirators and to store and publish stolen data.

Overt Act No. 12: On or about June 20, 2011, defendant CLEARY launched a DDoS attack against the servers hosting the website of Britain's Serious Organized Crime Agency.

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]

8. The Grand Jury re-alleges and incorporates by reference the allegations set forth in paragraphs one, two, and six of this Indictment.

9. On or about April 21, 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant CLEARY knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, a program, a system, and information on a computer system that was used in and affecting interstate and foreign commerce and communication, specifically, the computer systems of Fox Entertainment Group, Inc. ("Fox"), thereby causing a loss to Fox aggregating at least $5,000 in value during a one-year period beginning on or about April 21, 2011.

COUNT THREE

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I)]

10. The Grand Jury re-alleges and incorporates by reference the allegations set forth in paragraphs one, two, and six of this Indictment.

11. On or about April 30, 2011, in Los Angeles County, within the Central District of California, and elsewhere, defendant CLEARY knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, a program, a system, and information on a computer system that was used in and affecting interstate and foreign commerce and communication, specifically, DreamHost's computer systems, thereby causing a loss to DreamHost aggregating at least $5,000 in value during a one-year period beginning on or about April 30, 2011.

A TRUE BILL

/S/

Foreperson

ANDRÉ BIROTTE JR.
United States Attorney

ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division

WESLEY L. HSU
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

ERIC D. VANDEVELDE
Assistant United States Attorney
Deputy Chief, Cyber & Intellectual Property Crimes Section